SERVICE DESCRIPTION
FORTICARE TECHNICAL SUPPORT

1. Introduction

This document describes FortiCare Technical Support, which provides focused maintenance services aimed at operating and sustaining Fortinet products. It includes customer service and technical support assistance to resolve technical incidents, as well as software updates, access to on-line tools and the replacement of defective hardware.

2. Service Features and Descriptions

For the duration of the service, Fortinet will use commercially reasonable efforts to provide the customer with the features outlined below. There are two service levels available for purchase dependent on business requirements.

	8x5	24x7
Software updates	•	•
On-line support tools	•	•
Incident handling	•	•
Telephone support	•	•
Access to technical support 24x7		•
Advanced replacement hardware	•	•

Software updates

The customer will be entitled to software updates in the form of feature updates and maintenance releases. The customer may access such updates via password protected web access. This is subject to one copy per software release or signature file as appropriate, and is subject to, the Fortinet End-User License Agreement (EULA).

On-line support tools

The service includes access to Fortinet's technical support portal which provides access to software downloads, technical bulletins, asset management as well as the capability to log incidents with the Fortinet.

Technical support

During the duration of the service the customer will have access to Fortinet's Technical Assistance Center (TAC), which is staffed with customer service, technical support and hardware engineers and is available on a 24x7x365 day basis. Fortinet TAC engineers are experienced in trouble-shooting and will assist in the resolution of incidents, finding solutions and workarounds. Each regional TAC operates on a business day schedule of 09.00-18.00 (excluding public holidays), with telephone calls and incidents being routed globally, using a follow-the-sun mechanism.

By mutual agreement between the customer and Fortinet, technical tickets are assigned a priority, according to the following definitions:

- A Priority 1 ticket is an incident that causes a total loss or continuous instability of mission critical functionality in a live or production network environment, other examples are catastrophic impact to mission critical functionality impacting multiple active user sessions or a critical traffic impact, major loss of connectivity or a vital security flaw impacting active business services. The customer and Fortinet commit to dedicate technical resources 24 hours a day, 7 days a week, 365 days a year for Priority 1 Tickets. If a workaround is accepted a Priority 1 ticket will be reclassified in priority with the agreement of both parties. The customer can only create a Priority 1 ticket by telephoning Fortinet.
- A Priority 2 ticket is an incident that causes significant impact to mission critical functionality in a live or production network environment, other examples are serious loss or frequent instabilities of mission critical functionality impacting active user sessions, loss of redundancy of a critical component impacting live business services or a major security flaw has been identified impacting critical business services. The customer and Fortinet commit to

dedicate technical resources 8 hours a day, 5 days a week for Priority 2 Tickets. If the customer accepts a workaround, a Priority 2 ticket will be reclassified in priority, with the agreement of both parties. The customer can only create a Priority 2 ticket by telephoning Fortinet.

- A Priority 3 ticket is an incident that has minimal impact to business operations, examples are, occasional or intermittent instabilities of core functions, limited traffic impact or loss of connectivity. It may also cover the root cause analysis for a Priority 1 or Priority 2 ticket for which a workaround has been accepted. Fortinet and the customer will assign resources during business days until a resolution or workaround has been provided.
- A Priority 4 ticket is a created by the customer for additional information, including, basic configuration assistance, errors in documentation or minor defects which do not impact business services. Fortinet and the customer will assign resources during business days until a resolution or workaround has been provided.

For open tickets regular updates will be provided, containing either requests for additional information, or an incident resolution plan, as well as a description of any applicable workaround. For ticket handling the following goals exist to assure timely handling of incidents:

- A TAC engineer will provide an initial status update for Priority 1 and Priority 2 tickets within one hour of ticket creation. For Priority 3 tickets Fortinet will provide an initial status update on the next business day and for Priority 4 tickets Fortinet will provide an initial status update within the next two business days.
- Each technical ticket will be updated via a report on a regular basis containing the current status of the investigation. Each status update will be created by the TAC in accordance with the associated ticket priority; Priority 1 tickets every six hours, Priority 2 tickets once each calendar day, Priority 3 tickets every three business days, Priority 4 tickets once each calendar week.

An automatic notification to Fortinet management takes place if a ticket is not resolved in a timely manner. The notifications escalate through the Fortinet management chain as time progresses in accordance with the ticket priority.

Priority 1: TAC Manager: Immediately, VP Support: 6 Hours; VP Sales: 12 Hours, CEO, 24 hours
Priority 2: TAC Manager: Immediately, VP Support: 1 Business Day, VP Sales: 2 Business Days, CEO: 1 week
Priority 3: TAC Manager: 1 week, Regional Sales Director: 1 month
Priority 4: TAC Manager: 2 weeks, Regional Sales Director: 3 months

Hardware Replacements

The replacement of defective hardware is obtained by contacting the TAC with details of the incident. Upon confirmation of the hardware failure by Fortinet a replacement product will be provided which may be a new or reconditioned unit of equivalent or higher value. The following service goals exist:

- An Advanced Replacement product, will arrive on the next business day provided Fortinet's diagnosis of the problem and acceptance of the hardware defect is determined before 14:00 (local regional TAC time), otherwise the replacement will ship the next business day.

If Fortinet confirms a hardware failure within the first thirty (30 days) following a previous RMA shipment, this product is classified as a DOA-L (Dead on Arrival Logistic). For DOA-L products, Fortinet will bear the cost of shipment for the return of the defective product and process the request as an advanced replacement shipment.

6. Customer Requirements & Responsibilities

- Provide timely updates to open tickets; it should be noted that when a ticket is awaiting a customer response weekly reminders will be automatically initiated for a period of twenty calendar days. If after that time there has been no response from the customer, the ticket will be automatically closed.
- Ensure an up-to-date backup of the configuration is available to assist in the restoration of the product should that be required.
- To return defective product within thirty days after the receipt of the replacement unit. If the unit is not returned the customer agrees that Fortinet reserves the right to authorize invoicing at the then current list price of the product sent to replace the defective product, and that the Customer shall owe Fortinet payment according to such invoice, and that Fortinet shall be entitled, at Fortinet's discretion, to discontinue Services for the defective Product and/or replacement product until such defective product is received.

- Accepts that Fortinet is not responsible for transportation or custom delays. Customer compliance with export controls and destination customs processes may condition shipment times
- Agrees to assist in troubleshooting hardware problems prior to an RMA replacement being shipped by Fortinet.

By purchasing the service, the customer understands and agrees that Fortinet is not obligated to provide the service if they fail to meet these requirements.

7. Scope & Conditions

This document is applicable for technical support services that are rendered by Fortinet directly to the customer. Terms and conditions as outlined in the ''Fortinet Service Terms and Conditions'', (available on the Support Portal) and the EULA (http://www.fortinet.com/doc/legal/EULA.pdf) apply.

8. Eligibility & Purchasing

The service is available for purchase by a customer through authorized Fortinet resellers and distributors globally. The service is delivered to the customer of Fortinet products as referenced in the purchase order placed with Fortinet by a customer or Fortinet authorized partner or distributor.

The duration of the service is three hundred and sixty five days from activation per purchased service unit. The service may be cancelled by the end-user at any time and for any reason, but in no event will Fortinet refund any prepaid subscription fee. All sales are final

Purchasing Information: Refer to the pricelist for the specific product.